REMARKS

Upon entry of this amendment, claims 1-39, 41 and 42 are all the claims pending in the application. Claims 40 and 43 have been canceled by this amendment.

Applicants note that a number of editorial amendments have been made to the specification for grammatical and general readability purposes. No new matter has been added.

I. Double Patenting

In item 1 of the Office Action, the Examiner has rejected claims 1-7, 9-33, 37-40 and 43 because the Examiner believes that such claims conflict with claims 1-12, 14-32 and 36-51 of copending Application No. 10/725,102 application (hereafter "the '102 application"). As such, the Examiner has taken the position that Applicants are required to cancel the conflicting claims from all but one application (see Office Action at page 2). Applicants respectfully disagree with Examiner's position.

In particular, Applicants note that MPEP § 822, which is the section of the MPEP relied on by the Examiner, explicitly indicates that the requirement to cancel conflicting claims in copending applications should "be used when the conflicting claims are identical or conceded by applicant to be not patentably distinct" (emphasis added). In this regard, Applicants note that the claims identified by the Examiner in the present application and in the '102 application are not identical and, further, Applicants submit that such claims are patentably distinct.

For example, regarding claim 1 of the present application and claim 1 of the '102 application, Applicants note that claim 1 of the present application recites the feature of an encryption unit operable to encrypt the seed value based on the blind value to generate encryption information, whereas claim 1 of the '102 application recites the features of a first encryption unit operable to encrypt the verification value to generate first encryption information, and a second encryption unit operable to encrypt the seed value based on the verification value to generate second encryption information.

Further, Applicants note that claim 1 of the present application also recites the feature of a decryption unit operable to decrypt the encryption information to generate a decryption seed

value, whereas claim 1 of the '102 application recites the features of a first decryption unit operable to decrypt the first encryption information to generate a first decryption verification value, and a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value to generate a decryption seed value.

Moreover, Applicants note that claim 1 of the present application recites the feature of a judging unit operable to judge, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted, whereas claim 1 of the '102 application recites the feature of a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted.

In view of at least the foregoing differences recited in the claims, Applicants respectfully submit that claim 1 of the present application and claim 1 of the '102 application are clearly not identical, and further, that such claims are patentably distinct from one another due to such differences.

Accordingly, in view of the guidelines discussed above in MPEP § 822, because claim 1 of the present application and claim 1 of the '102 application are not identical, and because Applicants have not conceded that such claims are not patentably distinct, but instead, have set forth above how such claims are patentably distinct from one another, Applicants submit that the Examiner's above-noted requirement for Applicants to cancel claims is improper. Accordingly, Applicants kindly request that the Examiner reconsider and withdraw such a requirement.

Regarding independent claim 3 of the present application and independent claim 3 of the '102 application, Applicants note that claim 3 of the present application recites the feature of an encryption unit operable to encrypt the seed value based on the blind value to generate encryption information, whereas claim 3 of the '102 application recites the features of a first encryption unit operable to encrypt the verification value to generate first encryption information, and a second encryption unit operable to encrypt the seed value based on the verification value to generate second encryption information.

In view of at least the foregoing differences recited in the claims, Applicants respectfully submit that claim 3 of the present application and claim 3 of the '102 application are clearly not identical, and further, that such claims are patentably distinct from one another due to such differences. Accordingly, Applicants kindly request that the Examiner reconsider and withdraw such a requirement.

Regarding independent claim 21 of the present application and independent claim 24 of the '102 application, Applicants note that claim 21 of the present application recites the features of a decryption unit operable to decrypt the encryption information to generate a decryption seed value; and a judging unit operable to judge, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted, whereas claim 24 of the '102 application recites the features of a first decryption unit operable to decrypt the first encryption information to generate a first decryption verification value; a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value to generate a decryption seed value; and a judging unit operable to judge, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted.

For at least similar reasons as discussed above with respect to claim 1 of the present application and claim 1 of the '208 application, Applicants respectfully submit that claim 21 of the present application and claim 24 of the '102 application are not identical, and that such claims are patentably distinct from one another. As such, Applicants submit that the Examiner's above-noted requirement for Applicants to cancel claims is improper. Accordingly, Applicants kindly request that the Examiner reconsider and withdraw such a requirement.

Regarding independent claims 38 and 39 of the present application and independent claims 46 and 47 of the '102 application, Applicants note that claim 38 and 39 of the present application recite the feature of an encryption step of encrypting the seed value based on the blind value to generate encryption information, whereas claims 46 and 47 of the '102 application recite the features of a first encryption step of encrypting the verification value to generate first

encryption information, and a second encryption step of encrypting the seed value based on the verification value to generate second encryption information.

For at least similar reasons as discussed above with respect to claim 3 of the present application and claim 3 of the '102 application, Applicants respectfully submit that claims 38 and 39 of the present application and claims 46 and 47 of the '102 application are not identical, and that such claims are patentably distinct from one another. As such, Applicants submit that the Examiner's above-noted requirement for Applicants to cancel claims is improper. Accordingly, Applicants kindly request that the Examiner reconsider and withdraw such a requirement.

Regarding independent claims 41 and 42 of the present application and independent claims 49 and 50 of the '102 application, Applicants note that claim 41 and 42 of the present application recite the recite the features of a decryption step of decrypting the encryption information to generate a decryption seed value; and a judging step of judging based, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted, whereas claims 49 and 50 of the '102 application recite the features of a first decrypting step of decrypting the first encryption information to generate a first decryption verification value; a second decryption step of decrypting the second encryption information based on the first decryption verification value to generate a decryption seed value; and a judging step of judging, based on the first decryption verification value and the second decryption verification value, whether the decryption shared key should be outputted.

For at least similar reasons as discussed above with respect to claim 1 of the present application and claim 1 of the '102 application, Applicants respectfully submit that claims 41 and 42 of the present application and claims 49 and 50 of the '102 application are not identical, and that such claims are patentably distinct from one another. As such, Applicants submit that the Examiner's above-noted requirement for Applicants to cancel claims is improper. Accordingly, Applicants kindly request that the Examiner reconsider and withdraw such a requirement.

Regarding dependent claims 2, 4-7, 9-20, 22-33 and 37 of the present application, Applicants submit that these claims are patentably distinct from the claims in the '102

application for at least the same reasons as discussed above regarding independent claims 1, 3, 21, 38, 39, 41 and 42.

II. Claim Rejections under 35 U.S.C. § 101

The Examiner has rejected claims 39 and 42 under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Applicants have amended claims 39 and 42 so as to clarify that the program recited therein is embodied on a computer-readable storage medium. Accordingly, Applicants kindly request that the rejection be reconsidered and withdrawn.

III. Claim Rejections under 35 U.S.C. § 102

The Examiner has rejected claims 1-12, 16-29, 34-39, 41 and 42 under 35 U.S.C. § 102(b) as being anticipated by Hoffstein (WO/9808323). Applicants respectfully traverse this rejection on the following basis.

A. Claims 1, 2, 21-29, 34-37, 41 and 42

Claim 1 recites the features of a first shared-key generating unit operable to generate a blind value and a shared key, from the seed value; and a second shared-key generating unit operable to generate a decryption blind value and a decryption shared key, using the decryption seed value and according to a same method as used in the first-shared-key generating unit. Applicants respectfully submit that Hoffstein does not disclose or suggest such a combination of features.

Regarding Hoffstein, Applicants note that this reference discloses an encoding technique in which a secret key and a public key are generated by a first user (e.g., Dan) (see page 15, lines 23-25 and page 16, lines 7-12). As explained in Hoffstein, if a second user (e.g., Cathy) wants to send a message to Dan using his public key, she chooses a polynomial at random, and uses this polynomial, along with Dan's public key and her plaintext message, to create an encoded message to send to Dan (see page 16, lines 14-26).

In this regard, Applicants note that Fig. 2 of Hoffstein depicts the above-noted technique, in which the procedure begins at step 210 with Dan generating a public key and a private key,

and then publishing the public key (i.e., sending the public key to Cathy) (see page 22, lines 3-23). Next, in step 240, Cathy encodes a plaintext message using the public key generated by Dan, and the encrypted message is transmitted (see Fig. 2 and page 22, line 24 through page 23, line 4). Upon receipt of the encrypted message, Dan then decodes the encrypted message using his generated private key (see Fig. 2 and page 23, lines 5-11).

Thus, in Hoffstein, Dan first generates a public key and a private key, and then sends the public key to Cathy, whereby Cathy uses the public key generated by Dan to encrypt a message that is transmitted to Dan, and upon receipt of the encrypted message, Dan uses his private key to decrypt the encrypted message.

As noted above, claim 1 recites the features of a first shared-key generating unit operable to generate a blind value and a shared key from the seed value; and a second shared-key generating unit operable to generate a decryption blind value and a decryption shared key, using the decryption seed value and according to a same method as used in the first-shared-key generating unit.

With respect to the above-noted features, in the Office Action, the Examiner has apparently taken the position that the public key generated by Dan (as disclosed at pages 13-15 of Hoffstein) corresponds to the "shared key" that is generated by the "first shared-key generating unit" (see Office Action at page 15).

Regarding the "decryption shared key" that is generated by the "second shared-key generating unit ... according to a same method as used in the first shared-key generating unit", however, the Examiner has relied on the disclosure in Hoffstein at pages 17-18 as allegedly disclosing this feature (see Office Action at the top of page 16). With respect to the disclosure at pages 17-18 of Hoffstein, Applicants note that this section of Hoffstein merely relates to Dan decoding an encoded message received from Cathy by using his private key.

In other words, while the above-noted section in Hoffstein discloses the ability of Dan to decode an encrypted message using his private key, Applicants respectfully submit that such disclosure does not in any way whatsoever relate to the generation of a decryption blind value

and a decryption shared key according to the same method as used in the generation of the public key.

As such, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious the above-noted features of a first shared-key generating unit operable to generate a blind value and a shared key from the seed value; and a second shared-key generating unit operable to generate a decryption blind value and a decryption shared key, using the decryption seed value and according to a same method as used in the first shared-key generating unit, as recited in claim 1.

Accordingly, Applicants submit that claim 1 is patentable over Hoffstein, an indication of which is kindly requested.

Further, Applicants note that claim 1 also recites the features of a seed-value generating unit operable to generate a seed value; and an encryption unit operable to encrypt the seed value based on the blind value, to generate encryption information. Applicants respectfully submit that Hoffstein also does not disclose or suggest these features of claim 1.

In particular, in the Office Action, Applicants note that the Examiner has taken the position that Dan is responsible for generating the seed value, and then generating a public key from the seed value (see the Office Action at page 15). In this regard, as noted above, Dan sends the generated public key to Cathy so that Cathy can use this public key for sending encrypted data to Dan.

In the Office Action, however, the Examiner has also indicated that Cathy is responsible for encrypting "the seed value based on the blind value, to generate encryption information" (see Office Action at page 15). Applicants respectfully disagree.

In particular, Applicants note that while Cathy utilizes the public key generated by Dan when encoding a message that is to be sent to Dan, because Cathy does not generate the public key herself, it is clear that Cathy would not receive the seed value that is used by a first shared-key generating unit to generate the shared-key.

In view of the foregoing, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious the above-noted features of a seed-value generating unit

operable to generate a seed value; and an encryption unit operable to encrypt the seed value based on the blind value, to generate encryption information, as recited in claim 1.

Moreover, Applicants note that claim 1 also recites the feature a judging unit operable to judge, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted. In the Office Action, the Examiner has pointed to block 640 of Fig. 6 of Hoffstein as allegedly disclosing the above-noted feature (see the Office Action at page 16). Applicants disagree.

In particular, Applicants note that Fig. 6 of Hoffstein is a flow diagram depicting the routine for generating a public key and a private key (see the sentence bridging pages 25 and 26 of Hoffstein). With respect to block 640 of Fig. 6, Applicants note that this block merely represents the determination of previously defined matrices, and whether these matrices exist (see page 26 of Hoffstein).

As such, Applicants respectfully submit that while block 640 of Fig. 6 of Hoffstein is utilized in generating a public key and a private key, that this routine is not in any way related to a judgement, based on encryption information and re-encryption information, as to whether the decryption shared key should be output.

Accordingly, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious the above-noted feature recited in claim 1 of a judging unit operable to judge, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted.

In view of the foregoing, Applicants submit that claim 1 is patentable over Hoffstein, an indication of which is kindly requested. Claim 2 depends from claim 1 and is therefore considered patentable at least by virtue of its dependency.

Regarding claim 21, Applicants note that this claim is drawn to a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus, the shared-key generation apparatus generating a seed value, generating a shared key from the seed value, and encrypting the seed value to generate encryption information, wherein the shared-key recovery apparatus includes a decryption unit operable to decrypt the encryption information, to generate a

decryption seed value; a shared-key generating unit operable to generate a decryption blind value and a decryption shared key, using the decryption seed value and according to a same method as used in the shared-key generation apparatus; and a judging unit operable to judge, based on the encryption information and the re-encryption information, whether the decryption key should be outputted.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious such a combination of features. Accordingly, Applicants submit that claim 21 is patentable over Hoffstein, an indication of which is kindly requested.

Regarding claims 22-29 and 34-37, Applicants note that these claims depend from claim 24 and are therefore considered patentable at least by virtue of their dependency.

Regarding claims 41 and 42, Applicants note that these claims are drawn to a shared-key recovery method and program used in a shared-key recovery apparatus that receives a shared key from a shared-key generating apparatus, the shared-key generation apparatus generating a seed value, generating a shared key from the seed value, and encrypting the seed value to generate encryption information, wherein the shared-key recovery method includes a decryption step of decrypting the encryption information, to generate a decryption seed value; a shared-key generating step of generating a decryption blind value and a decryption shared key, using the decryption seed value and according to a same method as used in the shared-key generation apparatus; and a judging step of judging, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted.

For at least similar reasons as discussed above with respect to claim 1, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious such a combination of features. Accordingly, Applicants submit that claims 41 and 42 are patentable over Hoffstein, an indication of which is kindly requested.

B. Claims 3-12, 16-20, 38 and 39

Regarding claim 3, Applicants note that this claim recites the feature of a seed value-generating unit operable to generate a seed value; a shared-key generating unit operable to generate a blind value and a shared key, from the seed value; and an encryption unit operable to encrypt the seed value based on the blind value, to generate encryption information. Applicants respectfully submit that Hoffstein does not disclose or suggest such a combination of features.

In the Office Action, Applicants note that the Examiner has taken the position that Dan is responsible for generating the seed value, and then generating a public key from the seed value (see the Office Action page 17). In this regard, as noted above, Dan sends the generated public key to Cathy so that Cathy can use this public key for sending encrypted data to Dan.

In the Office Action, however, the Examiner has also indicated that Cathy is responsible for encrypting "the seed value based on the blind value, to generate encryption information" (see Office Action at page 17). Applicants disagree.

In particular, as discussed above, Applicants note that while Cathy utilizes the public key generated by Dan when encoding a message that is to be sent to Dan, because Cathy does not generate the public key herself, it is clear that Cathy would not receive the seed value that is used to by a shared-key generating unit to generate the shared key.

In view of the foregoing, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious the above-noted combination of features of a seed value-generating unit operable to generate a seed value; a shared-key generating unit operable to generate a blind value and a shared key, from the seed value; and an encryption unit operable to encrypt the seed value based on the blind value, to generate encryption information.

Accordingly, Applicants submit that claim 3 is patentable over Hoffstein, an indication of which is kindly requested. Claim 4-12 and 16-20 depend from claim 3 and are therefore considered patentable at least by virtue of their dependency.

Regarding claims 38 and 39, Applicants note that each of these claims recites the features of a seed-value generating step of generating a seed value; a shared-key generating step of generating a blind value and shared key, from the seed value; and an encryption step of encrypting the seed value based on the blind value, to generate the encryption information.

For at least similar reasons as discussed above with respect to claim 3, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious such a combination of features. Accordingly, Applicants submit that claims 38 and 39 are patentable over Hoffstein, an indication of which is kindly requested.

IV. Claim Rejections under 35 U.S.C. § 103(a)

The Examiner has rejected claims 13-15, 30-33, 40 and 43 under 35 U.S.C. § 103(a) as being unpatentable over Hoffstein (WO/9808323).

Claims 13-15 depend from claim 3; and claims 30-33 depend from claim 21. As discussed above, Applicants respectfully submit that Hoffstein does not disclose, suggest or otherwise render obvious all of the features recited in claims 3 and 21. Accordingly, Applicants submit that claims 13-15 and 30-33are patentable at least by virtue of their dependency.

V. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Masato YAMAMICHI et al.

By: Kenneth W. Fields

Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/jjv
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
April 19, 2007